Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

05.03.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.49 Безопасность операционных систем

1. Код и наименование направления подготовки:

10.03.01 Информационная безопасность

2. Профиль подготовки:

Направленность (профиль) N 1 "Безопасность компьютерных систем" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника:

Бакалавр

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра информационных систем

6. Составители программы:

Савинков Андрей Юрьевич, д.т.н., профессор

7. Рекомендована:

НМС ФКН, протокол № 5 от 05.03.2025

8. Учебный год:

2027-2028

9.Цели и задачи учебной дисциплины:

Обучение студентов принципам построения защиты информации в ОС и анализа надежности их защиты.

Основные задачи дисциплины:

- получение базовых знаний о принципах построения подсистем защиты в ОС различной архитектуры;
- знакомство со средствами и методами несанкционированного доступа к ресурсам ОС;
- выработка системного подхода к проблеме защиты информации в ОС;
- овладение механизмами защиты информации и изучение возможностей по их преодолению.

10. Место учебной дисциплины в структуре ООП:

Дисциплина обязательной части (Б1.О). Входные знания: «Операционные системы»

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;	ОПК-1.1.1 знает архитектуру и принципы построения и защиты операционных систем	Знает архитектуру и принципы построения защиты операционных систем
ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;	ОПК-1.1.2 знает программные интерфейсы настроек политик управления доступом в операционных системах	Знает программные интерфейсы настроек политик управления доступом в операционных системах UNIX, FreeBSD, GNU/Linux и MS Windows
ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;	ОПК-1.1.3 умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации	Умеет использовать встроенные средства защиты информации операционных систем GNU/Linux и MS Windows для противодействия угрозам безопасности информации
ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;	ОПК-1.1.4 владеет навыками настройки антивирусной защиты при обеспечении безопасности операционных систем	Владеет навыками настройки антивирусной защиты и сетевого экрана операционных систем GNU/Linux и MS Windows

12. Объем дисциплины в зачетных единицах/час:

2/72

Форма промежуточной аттестации:

Зачет с оценкой

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 6	Всего
Аудиторные занятия	60	60
Лекционные занятия	30	30
Практические занятия	0	0
Лабораторные занятия	30	30
Самостоятельная работа	12	12
Курсовая работа	0	0
Промежуточная аттестация	0	0
Часы на контроль	0	0
Всего	72	72

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основы защиты информации в операционных системах	Общие требования к защите информации, технические и административные методы защиты, уровни доверия, политики безопасности, профили защиты	https://edu.vsu.ru/course/view.php?id=15499
1.2	Управление доступом	Объекты, субъекты и методы доступа, модели управления доступом, изолированная программная среда	https://edu.vsu.ru/course/view.php?id=15499
1.3	Аутентификация пользователей и проверка целостности информации	Факторы аутентификации, хранение паролей, аутентификация по открытому каналу, одноразовые пароли, многофакторная аутентификация	https://edu.vsu.ru/course/view.php?id=15499
1.4	Разграничение доступа в Unix и Unix-подобных системах	Базовая модель разграничения доступа в UNIXподобных системах, учет пользователей и хранение паролей, регистрация пользователей и вход в систему, PAM	https://edu.vsu.ru/course/view.php?id=15499
1.5	Методы защиты информации в Linux	Возможности (capabilities) потоков в Linux, управление возможностями, списки контроля доступа Linux, дополнительные атрибуты файлов, изоляция (пространства имен) в Linux, система sudo, seccomp, SELinux, AppArmor	https://edu.vsu.ru/course/view.php?id=15499

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.6	Методы защиты информации в Windows	Дескрипторы защиты и маркеры доступа, олицетворение, списки контроля доступа в Windows	https://edu.vsu.ru/course/view.php?id=15499
1.7	Основы сетевой безопасности	Межсетевой экран Linux и Windows	https://edu.vsu.ru/course/view.php?id=15499
1.8	Аудит в операционных системах	Журналы аудита Linux и Windows, фильтры аудита	https://edu.vsu.ru/course/view.php?id=15499
2. Практические занятия			
3. Лабораторные работы			
3.1	Управление пользователями в Linux	Создание учетной записи, присоединение к группе, замена программы (оболочки) пользователя, создание псевдопользователя для запуска программы	https://edu.vsu.ru/course/view.php?id=15499
3.2	Контроль целостности файлов в Linux	Вычисление и проверка контрольной суммы, проверка целостности программы при запуске	https://edu.vsu.ru/course/view.php?id=15499
3.3	Изучение PAM	Реализация модуля PAM, реализующего аутентификацию по серийному номеру устройства USB	https://edu.vsu.ru/course/view.php?id=15499
3.4	Изучение возможностей (capabilities) Linux	Установка возможностей программы для выполнения привилегированных действий без использования root	https://edu.vsu.ru/course/view.php?id=15499

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3.5	Изучение изоляции ресурсов Linux	Создание изолированной сетевой среды, создание сетевого туннеля для доступа к изолированной среде, утилита unshare, файловая система /sys/fs/cgroup/	https://edu.vsu.ru/course/view.php?id=15499
3.6	Изучение подсистемы sudo	Создание правила для конкретного пользователя	https://edu.vsu.ru/course/view.php?id=15499
3.7	Изучение подсистемы seccomp	Ограничение запуска программ и доступа к файлам за счет реализации фильтра системных вызовов	https://edu.vsu.ru/course/view.php?id=15499
3.8	Изучение межсетевого экрана Linux	Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам	https://edu.vsu.ru/course/view.php?id=15499
3.9	Изучение механизмов ограничения запуска программ в Windows	Создание правил политики ограничения запуска программ	https://edu.vsu.ru/course/view.php?id=15499
3.10	Изучение межсетевого экрана Windows	Создание правил для Брэндмауэра, ограничивающих доступ к отдельным сетевым протоколам и портам	https://edu.vsu.ru/course/view.php?id=15499

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Основы защиты информации в операционных системах	4	0	0	0	4
2	Управление доступом	2	0	0	0	2
3	Аутентификация пользователей и проверка целостности информации	4	0	0	0	4

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
4	Разграничение доступа в Unix и Unix-подобных системах	4	0	0	1	4
5	Методы защиты информации в Linux	4	0	0	0	4
6	Методы защиты информации в Windows	4	0	0	0	4
7	Основы сетевой безопасности	4	0	0	0	4
8	Аудит в операционных системах	4	0	0	0	4
9	Управление пользователями в Linux	0	0	2	1	3
10	Контроль целостности файлов в Linux	0	0	2	1	3
11	Изучение PAM	0	0	4	2	6
12	Изучение возможностей (capabilities) Linux	0	0	2	1	3
13	Изучение изоляции ресурсов Linux	0	0	4	2	6
14	Изучение подсистемы sudo	0	0	4	1	5
15	Изучение подсистемы seccomp	0	0	2	1	3
16	Изучение механизмов ограничения запуска программ в Windows			2	1	3
17	Изучение межсетевого экрана Linux	0	0	4	1	5
18	Изучение межсетевого экрана Windows	0	0	4	1	5
		30	0	30	12	72

14. Методические указания для обучающихся по освоению дисциплины

Дисциплина требует работы с файлами-презентациями лекций и соответствующими главами рекомендованной основной литературы, а также, обязательного выполнения всех лабораторных заданий в компьютерном классе.

Самостоятельная работа проводится в компьютерных классах ФКН с использованием методических материалов расположенных на учебно-методическом сервере ФКН "\\fs.cs.vsu.ru\Library" и на сервере Moodle ВГУ moodle.vsu.ru, выполнением задач конфигурирования виртуализированной ИС. Во время самостоятельной работы студенты используют электронно-библиотечные системы, доступные на портале Зональной Библиотеки ВГУ по адресу www.lib.vsu.ru. Часть заданий может быть выполнена вне аудиторий на домашнем компьютере, после копирования методических указаний и необходимого ПО с учебно-методического сервера ФКН.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимыхдля освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Технологии обеспечения безопасности информационных систем: учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. // ЭБС Университетская библиотека. – URL: https://biblioclub.ru/index.php?page=book_red&id=598988

б) дополнительная литература:

№ п/п	Источник
1	Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с. // ЭБС Университетская библиотека. – URL: https://biblioclub.ru/index.php?page=book&id=438331

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Библиотека ВГУ, http://www.lib.vsu.ru
2	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
3	Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
2	Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Лекции-визуализации с демонстрацией иллюстративных и графических материалов, анимации, блок-схем алгоритмов и примеров исходного кода, демонстрацией выполнения команд операционной системой, лабораторные работы.

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1. Лекционная аудитория, оснащенная видеопроектором.
2. Компьютерный класс для проведения лабораторных занятий, оснащенный видеопроектора и компьютерами с операционной системой GNU/Linux.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Основы защиты информации в операционных системах Аутентификация пользователей и проверка целостности информации Основы сетевой безопасности Аудит в операционных системах	ОПК-1.1	ОПК-1.1.1	Собеседование
2	Управление доступом Разграничение доступа в Unix и Unix-подобных системах Методы защиты информации в Linux Методы защиты информации в Windows	ОПК-1.1	ОПК-1.1.2	Собеседование
3	Управление пользователями в Linux Контроль целостности файлов в Linux Изучение PAM Изучение возможностей (capabilities) Linux Изучение подсистемы sudo	ОПК-1.1	ОПК-1.1.3	Лабораторные работы, Контрольная работа
4	Изучение подсистемы seccomp Изучение механизмов ограничения запуска программ в Windows Изучение межсетевого экрана Linux Изучение межсетевого экрана Windows	ОПК-1.1	ОПК-1.1.4	Лабораторные работы, Контрольная работа

Промежуточная аттестация

Форма контроля - Зачет с оценкой

Оценочные средства для промежуточной аттестации

Собеседование

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль успеваемости выполняется по лабораторным работам.

Темы лабораторных работ

1. Управление пользователями в Linux
2. Контроль целостности файлов в Linux
3. Изучение PAM
4. Изучение возможностей (capabilities) Linux
5. Изучение изоляции ресурсов Linux
6. Изучение подсистемы sudo
7. Изучение подсистемы seccomp
8. Изучение механизмов ограничения запуска программ в Windows

9. Изучение межсетевого экрана Linux
10. Изучение межсетевого экрана Windows

По каждой выполненной работе должен быть предоставлен отчет, включающий исходный код разработанных программ (скриптов) и описание полученных результатов. По отчету преподаватель вправе задать дополнительные вопросы для уточнения уровня понимания материала. Лабораторная работа оценивается максимум в 100 баллов.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ОПК-1

Задания закрытого типа

1) Какие из перечисленных далее методов защиты информации относятся к техническим методам защиты
   a) Разработка политики безопасности
   b) Контроль целостности информации
   c) Разграничение доступа
   d) Создание и хранение резервных копий ценной информации
   e) Криптографическая защита
   f) Аудит безопасности
2) Псевдопользователи в UNIX и UNIX-подобных системах это
   a) Зарегистрированные пользователи (есть учетная запись в системе), которые не ассоциируются с человеком
   b) Пользователи, работающие в системе удаленно
   c) Пользователи, доступ которых в систему временно ограничен
   d) Низкоквалифицированные пользователи
3) Операционная система называется защищенной, если
   a) Назначен системный администратор
   b) Она не подключена к сети Интернет
   c) В ней реализованы средства защиты информации
4) Использование модели управления доступом типа изолированная программная среда обеспечивает
   a) Существенное повышение защищенности от программных закладок по сравнению с дискреционной моделью
   b) Высокую надежность защиты от утечки информации
5) Перечислите пункты, определяющие общие требования к защите информации
   a) Сохранение количества информации
   b) Сохранение целостности информации
   c) Сохранение формата представления информации
   d) Сохранение доступности информации
   e) Сохранение конфиденциальности информации

Ответы на вопросы

Номер вопроса	Ответ (буква)
1	b,c,e,f
2	a
3	c
4	a
5	b,d.e

Задания открытого типа

1) Сколько методов доступа различается в традиционной модели разграничения доступа UNIX
2) Напишите команду, чтобы назначить пользователя ivan владельцем файла с именем file в текущем каталоге

Ответы на вопросы

Номер вопроса	Ответ
1	3
2	chown ivan file или chown ivan ./file

Задания с развёрнутым ответом

1) Дайте определение политики безопасности
2) Дайте определение права доступа

Ответы на вопросы

Номер вопроса	Ответ (буква)
1	Политика безопасности – это набор правил, регламентирующих порядок хранения и обработки информации

Критерии оценивания	Шкала оценок (в баллах)
Обучающийся дал правильное определение политики безопасности	3 балла
Обучающийся дал правильное определение политики безопасности. Ответ содержит незначительные неточности	2 балла
Обучающийся дал не точное определение политики безопасности. Ответ не содержит грубых ошибок или неточностей	1 балл
Обучающийся дал не точное определение политики безопасности. Ответ содержит грубые ошибки и неточности	0 баллов

Номер вопроса	Ответ (буква)
2	Право доступа – это возможность субъекта доступа выполнять доступ к объекту доступа по некоторому методу доступа

Критерии оценивания	Шкала оценок (в баллах)
Обучающийся дал правильное определение права доступа	3 балла
Обучающийся дал правильное определение права доступа. Ответ содержит незначительные неточности	2 балла
Обучающийся дал не точное определение права доступа. Ответ не содержит грубых ошибок и неточностей	1 балл
Обучающийся дал не точное определение права доступа. Ответ содержит грубые ошибки или неточности	0 баллов

20.2 Промежуточная аттестация

Перечень вопросов к собеседованию

1. Общие требования к защите информации. Технические и административные методы защиты.
2. Политика безопасности.
3. Уровень доверия. Оценочные уровни доверия. Профиль защиты.
4. Управление доступом. Объекты, субъекты, методы доступа. Право доступа. Привилегия. Полномочия. Роль. Суперпользователь.

5. Типовые модели управления доступом (дать общее определение дискреционного управления доступом, мандатного управление доступом и изолированной программной среды)
6. Дискреционное управление доступом. Матрица доступа. Мандат возможностей. Список контроля доступа.
7. Мандатное управление доступом. Модель Белла-Лападулы.
8. Изолированная программная среда.
9. Аутентификация пользователей. Факторы аутентификации. Одноразовый пароль.
10. Многофакторная аутентификация. Хранение паролей.
11. Алгоритм проверки целостности HMAC.
12. Аутентификация HOTP на основе одноразовых паролей.
13. Аутентификация TOTP на основе одноразовых паролей.
14. Алгоритм OCRA - алгоритм взаимной аутентификации на основе взаимодействия запрос-ответ.
15. Базовая модель разграничения доступа в UNIX-подобный системах. Маска доступа для файлов и каталогов.
16. Учет пользователей в UNIX-подобный системах. Файл /etc/passwd. Учет групп. Хранение паролей в UNIX-подобный системах.
17. Псевдопользователи. Стандартные пользователи и группы в UNIX-подобный системах. Создание нового пользователя.
18. Файлы конфигурации системы учета пользователей в Linux. Инициализация домашнего каталога нового пользователя. Стандартные утилиты управления учетными записями в Linux.
19. Linux: Вход пользователя в систему.
20. PAM. Модули PAM. Конфигурация PAM. Критерии успешной аутентификации. Расширенный стиль конфигурации в Linux.
21. Списки контроля доступа и дополнительные атрибуты файлов в файловых системах Linux.
22. Система sudo. Правила sudo. Файл sudoers. Журнал sudo.
23. Обязательный контроль целостности и контроль учетных записей в Windows
24. Ограничение использования приложений в Windows
25. Межсетевой экран Linux
26. Межсетевой экран Windows
27. Аудит безопасности в Linux
28. Аудит безопасности в Windows

Описание технологии проведения

Собеседование производится в форме устного ответа на заданный вопрос. При необходимости преподаватель может задавать уточняющие вопросы.

Примеры КИМ

Контрольно-измерительный материал № 1

1. Общие требования к защите информации. Технические и административные методы защиты.

2. Изолированная программная среда.

Контрольно-измерительный материал № 2

1. Политика безопасности.

2. Списки контроля доступа и дополнительные атрибуты файлов в файловых системах Linux.

Контрольно-измерительный материал № 3

1. Уровень доверия. Оценочные уровни доверия. Профиль защиты.

2. Межсетевой экран Linux.

Контрольно-измерительный материал № 4

1. Аутентификация пользователей. Факторы аутентификации. Одноразовые пароли.

2. Списки контроля доступа и дополнительные атрибуты файлов в файловых системах Linux.

Требования к выполнению заданий, шкалы и критерии оценивания

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины, осуществляется в ходе текущей и промежуточной аттестаций. При оценивании результатов промежуточной аттестации используется количественная шкала оценок. Оценки за лабораторные работы складываются с оценкой, полученной на собеседовании, результат нормируется к 100 бальной шкале. Полученное значение определяет уровень сформированности компетенций и итоговую оценку (достаточный – удовлетворительно, хорошо, отлично или недостаточный – неудовлетворительно) согласно следующей шкале:

- оценка «отлично» – 90…100 баллов
- оценка «хорошо» – 70…89 баллов
- оценка «удовлетворительно» – 50...69 баллов
- оценка «неудовлетворительно» – 0...49 баллов